State Information Technology Security Policy

1. **PURPOSE**

To establish a statewide security policy for the protection of Information Technology (IT) assets and resources for the State of South Carolina.

2. **SCOPE**

This Policy applies to agencies, departments, commissions, and boards (herein referred to as "agencies") that receive, expend or disburse State funds or incur obligations for the State. This policy does not apply to colleges and universities. However, they are encouraged to comply due to the frequent need to access and exchange data with the agencies.

The agency's assigned Designated Approving Authority (DAA), working in conjunction with the Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of statewide information technology policies, standards, and procedures within each agency.

3. **POLICY**

The State of South Carolina shall securely and economically protect its business functions, including public access to appropriate information and resources, while maintaining compliance with the legal requirements established by existing Federal and State statutes pertaining to confidentiality, privacy, accessibility, availability, and integrity.

3.1. The policy establishes that:

- Agencies are responsible for providing security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, modification to, or destruction of either 1) information collected or maintained by or on behalf of the Agency or 2) information systems used by an Agency or by a contractor of an Agency or other organization on behalf of the Agency.
- Agencies shall ensure that networks, hardware systems, and software application systems operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.
- Agencies shall ensure that adequate security is provided for all information collected, processed, transmitted, stored, or disseminated in Agency software application systems.
- Levels of security applied to information systems and resources shall be commensurate with the value of the information being protected.
- Security controls applied to information systems and resources shall be sufficient to contain risk of loss or misuse of the information.
- Agencies are responsible for ensuring that information security management processes are integrated with Agency strategic and operational planning processes.

- Security architecture shall be based on industry-wide, open standards, and where possible, accommodate varying levels of security.
- Inter-Agency IT security components protecting critical Agency and State systems must be interoperable.
- Agencies are responsible for ensuring that staff is adequately trained in information security awareness.

3.2. Each Agency will have a comprehensive, documented set of policies that are periodically reviewed and updated. These policies address key security topic areas, including:

- Security strategy and management
- Security risk management
- Physical security
- System and network management
- System administration tools
- Monitoring and auditing
- Authentication and authorization
- Vulnerability management
- Encryption
- Security architecture and design
- Incident management
- Staff security practices
- Applicable laws and regulations
- Awareness and training
- Collaborative information security
- Contingency planning and disaster recovery

3.3. Agency shall assess their Technology Security by:

- Utilizing self assessments that adhere to industry-accepted best practices.
- Web-based reviews are offered by the CIO to ensure Agency compliance with best practices. Data from these reviews will be warehoused and accessible at the CIO.